添付資料

【今月の呼びかけ】

「 無線 LAN を他人に使われないようにしましょう！ 」

近年、一般家庭の無防備な無線 LAN 環境が悪用されるといった事件が複数報道されています。セキュリティ設定が不十分な無線 LAN 環境は、悪意ある者に使われてしまう危険性があります。実際に、一般家庭の無防備な無線 LAN 環境などを含む様々な犯罪インフラ※が、国内の組織犯罪、詐欺、窃盗、サイバー犯罪等のあらゆる犯罪の分野で着々と構築され、巧妙に張り巡らされてきているという現状があります。警察庁は、2011 年 3 月 10 日に、犯罪インフラへの対策の指針となる「犯罪インフラ対策プラン」を策定するなど、取り締まりを強化する方針を打ち出しました。

自宅の無線 LAN が犯罪インフラとして悪用されないよう、セキュリティ設定を適切に行ってください。

※ 犯罪インフラとは犯罪を助長し、又は容易にする基盤のこと。基盤そのものは合法であっても、犯罪に悪用されている状態にあれば、犯罪インフラとなる。

（ご参考）
犯罪インフラ対策プラン（警察庁）
http://www.npa.go.jp/sosikihanzai/kikakubunseki/bunseki/taisakuplan.pdf

（1）無線 LAN を取り巻く問題の概要

無線 LAN は、電波を使って無線 LAN アクセスポイント（以下、「親機」）と無線 LAN 機能を持つパソコン、スマートフォン、一部のゲーム機など（以下、「子機」）との間で通信を行うネットワーク環境のことです。無線 LAN では親機と子機の双方に通信のための設定をすることで、電波の届く範囲であれば、壁などの障害物を越えて通信が可能となります。

無線 LAN は便利であると同時に、家庭内ネットワークへの侵入や、インターネットでの不正行為のいわゆる「踏み台」など、悪用の対象として狙われやすいものです。電波という目に見えない通信経路を使うということは、侵入されていることさえも気付きにくいため、注意が必要です（図 1-1 参照）。

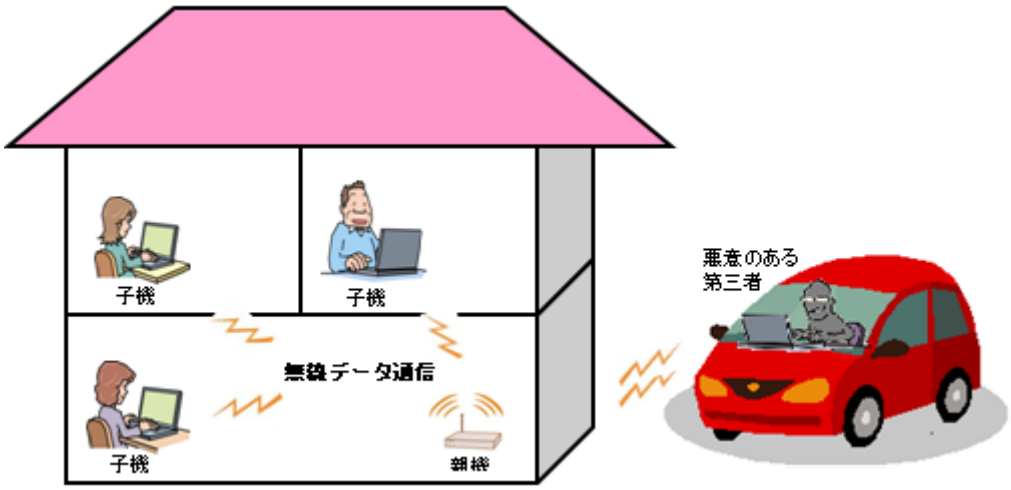


図 1-1：無線 LAN を取り巻く脅威のイメージ

（2）無線 LAN が関係した事件の実例

無線 LAN が関係した事件の実例を、表 1-1 に示します。

表 1-1：無線 LAN が関係した事件の実例

時期	内容
2008 年 6 月	インターネットに接続できる携帯ゲーム機を使用して他人の家の無線 LAN に無断で接続し、インターネットの掲示板に無差別殺人をほのめかす書き込みをしたとして、男が逮捕された。
2008 年 10 月	インターネットオークションで、児童ポルノの DVD を販売したとして逮捕された男が、他人の家の無線 LAN に無断で接続し、児童ポルノのファイルを入手していた。
2010 年 2 月	他人の家の無線 LAN に無断で接続し、あらかじめ不正に入手していた他人のクレジットカード情報を使用してインターネットで買い物をしたとして、詐欺グループのメンバー2 人が逮捕された。
2010 年 6 月	インターネットの掲示板に銀行口座を販売するなどと書き込み、現金を騙し取ったとして逮捕された男が、身元が特定できないように他人の家の無線 LAN から無断でインターネットに接続していた。

これらの実例はいずれも、無線 LAN のセキュリティ設定が不十分だったために、自宅の無線 LAN 環境を無断で使用されて、「踏み台」として悪用されてしまったケースです。これ以外にも想定される被害として、以下のようなことが考えられます。

・無線 LAN 環境に侵入され、重要な情報を盗まれる。
・通信データを盗聴される。

（3）対策

上記のような被害に遭わないためには、無線 LAN におけるセキュリティ設定が重要となりますが、そのポイントは「適切な暗号化方式の選択」と「適切なパスワードの設定」の 2 点になります。

（i）適切な暗号化方式の選択

無線 LAN の暗号化方式には大きく分けて、「**WEP**」、「**WPA**」、「**WPA2**」の 3 種類があり、最も安全な暗号化方式はこの中で最新の「WPA2」です。

「WPA2」の中にもいくつか種類がありますので、実際に暗号化方式を選択する場合、WPA2-PSK（Pre-Shared Key）という認証方式を利用したもののうち、最もセキュリティ強度が高い「**WPA2-PSK（AES）**」を選択してください。

これが選択できない場合は次善策として「WPA」の中から、WPA-PSK（Pre-Shared Key）という認証方式を利用したもののうち、最もセキュリティ強度が高い「**WPA-PSK（AES）**」を選択してください。

それ以外の暗号化方式ではセキュリティ強度が十分でないため、選択しないでください。なお、暗号化方式の詳しい説明については、以下のウェブページに記載しています。

（ご参考）
IPA――一般家庭における無線 LAN のセキュリティに関する注意
http://www.ipa.go.jp/security/ciadr/wirelesslan.html

参考として、図 1-2 に親機の設定画面例を、図 1-3 に設定状態の確認画面例を示します。無線 LAN の利用者は、念のため自宅の無線 LAN の設定を確認してください。なお、画面や確認方法、設定方法は機種によって異なります。操作等については、親機の取扱説明書を参照してください。

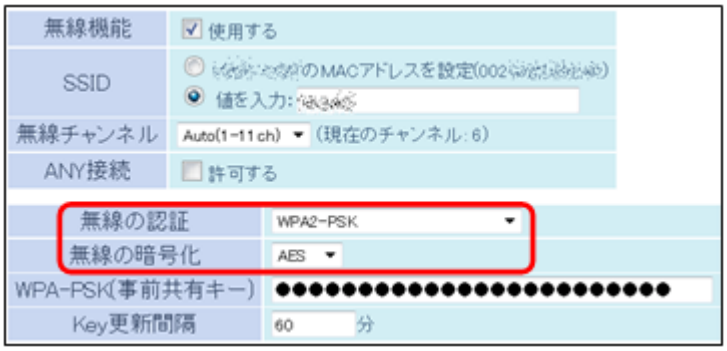


図 1-2：親機の設定画面例

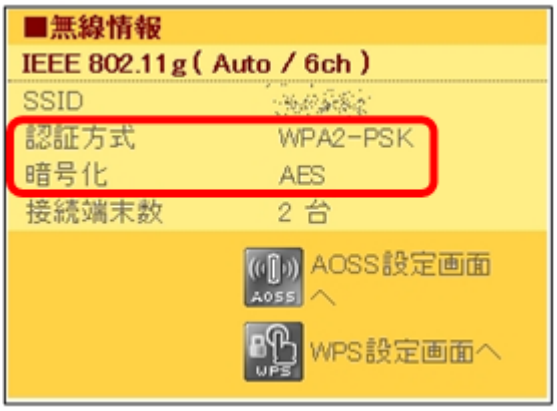


図 1-3：親機の設定状態の確認画面例

なお、**親機と全ての子機が、選択したい暗号化方式に対応していなければなりません。**つまり、親機を「WPA2-PSK（AES）」に設定した場合は、その親機に接続されている全ての子機を「WPA2-PSK（AES）」に設定する必要があります。

（ii）適切なパスワードの設定

上記の暗号化方式で使用する暗号鍵を生成するために、パスワードの設定が必要となります。パスワードを設定する際は、容易に推測されることを防ぐため、以下の注意事項に従ってください。

- 英語の**辞書に載っている単語を使用しない**
- **大文字、小文字、数字、記号の全てを含む**文字列とする
  文字数は**最低でも 20 文字**（半角英数字＋記号の場合。最大で 63 文字）とする